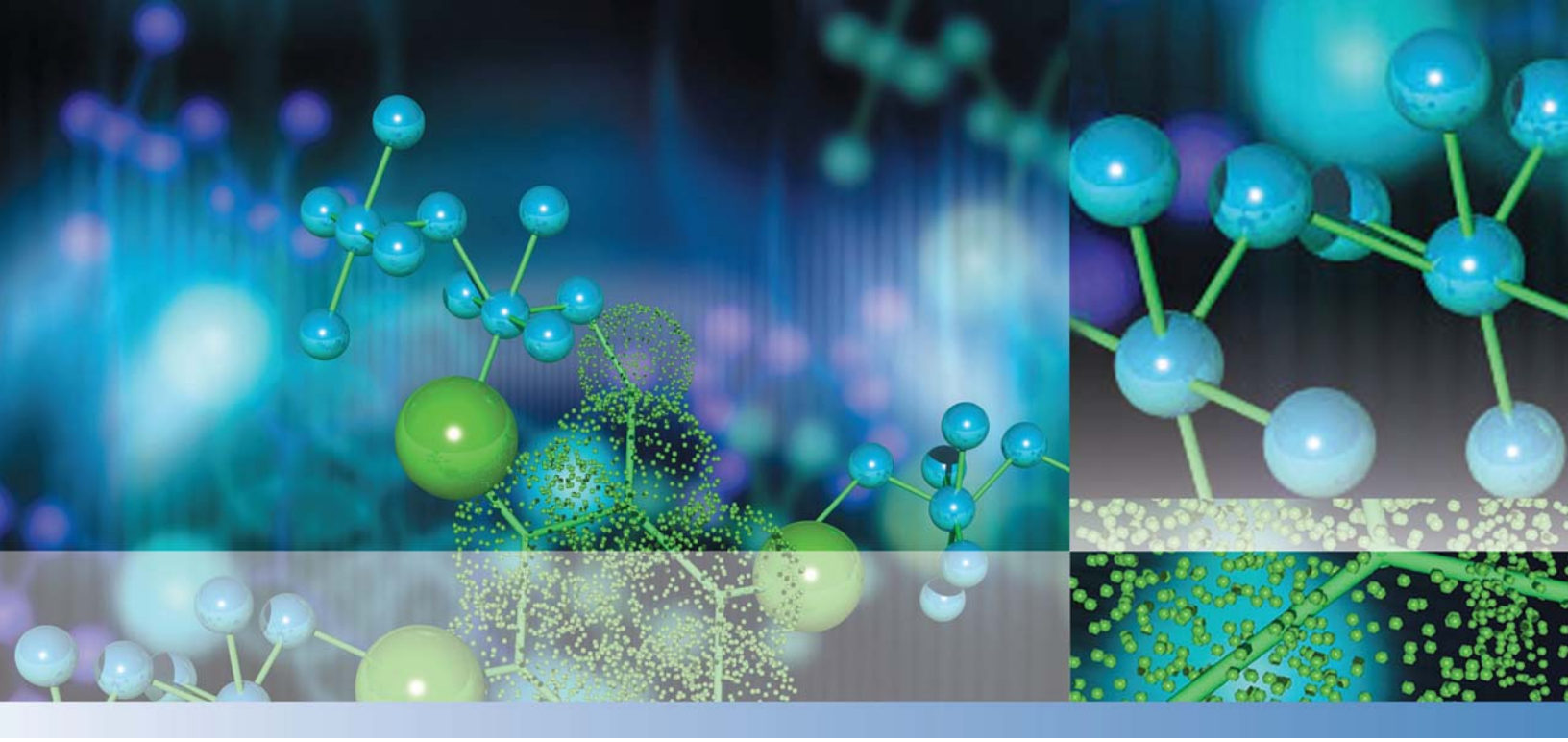


Thermo

# ToxFinder

## Administrator Console User Guide

Software Version 1.0

XCALI-97689 Revision A August 2014

DOCUMENTATION SURVEY

Thermo SCIENTIFIC

© 2014 Thermo Fisher Scientific Inc. All rights reserved.

ToxFinder and Foundation are trademarks, and Xcalibur is a registered trademark of Thermo Fisher Scientific Inc. in the United States.

Apache and OpenOffice are trademarks of the Apache Software Foundation.

NIST is a registered trademark of the National Institute of Standards and Technology in the United States.

The following are registered trademarks in the United States and other countries: Windows, Active Directory, Excel, and Microsoft are registered trademarks of Microsoft Corporation. Adobe, Acrobat, and Reader are registered trademarks of Adobe Systems Inc.

All other trademarks are the property of Thermo Fisher Scientific Inc. and its subsidiaries.

Thermo Fisher Scientific Inc. provides this document to its customers with a product purchase to use in the product operation. This document is copyright protected and any reproduction of the whole or any part of this document is strictly prohibited, except with the written authorization of Thermo Fisher Scientific Inc.

The contents of this document are subject to change without notice. All technical information in this document is for reference purposes only. System configurations and specifications in this document supersede all previous information received by the purchaser.

This document is not part of any sales contract between Thermo Fisher Scientific Inc. and a purchaser. This document shall in no way govern or modify any Terms and Conditions of Sale, which Terms and Conditions of Sale shall govern all conflicting information between the two documents.

Release history: Revision A, August 2014

Software version: Microsoft Windows 7 Professional; (Thermo) Foundation 3.0 SP2; Xcalibur 2.2 SP1

**For Research Use Only. Not for use in diagnostic procedures.**

# Contents

**Preface** . . . . . **v**

**Chapter 1** **Using the Security View** . . . . . **1**
Authentication Provider . . . . . 1
Global Policy . . . . . 3
Users . . . . . 6
Roles . . . . . 7
Role Mapping . . . . . 14

**Chapter 2** **Using the Repository View** . . . . . **17**
Administration . . . . . 17
Domain Mapping . . . . . 20

**Chapter 3** **Using the Plugins View** . . . . . **21**

**Chapter 4** **Importing and Exporting Administrator Settings** . . . . . **23**

**Index** . . . . . **25**

# Preface

This guide discusses the features of the Thermo ToxFinder™ Administrator Console. This console is available to any user with Administrator permissions.

If you are a member of the local administrator's group and are launching the ToxFinder application for the first time, you will have Administrator permissions. See "Role Permission Defaults" on page 13.

**Contents**


- Related Documentation
- System Requirements
- Special Notices
- Contacting Us
- Accessing the Administrator Console


## Related Documentation

The ToxFinder application includes complete documentation. In addition to this guide, you can also access the following documents as PDF files from the data system computer:

- *ToxFinder User Guide*
- *ToxFinder Data Review Quick Reference Guide*
- *ToxFinder Shortcut Menus Quick Reference Guide*

❖ **To view the product manuals**

From the Microsoft™ Windows™ taskbar, choose **Start > All Programs > Thermo ToxFinder > Manuals**.

For access to the application Help, follow this procedure.

❖ **To view the ToxFinder application Help**

- From the application window, choose **Help > ToxFinder Help**.
- If information about setting parameters is available for a specific view, page, or dialog box, click the **Help** icon, .

For more information, visit www.thermoscientific.com.

# System Requirements

The ToxFinder application requires a license. In addition, ensure that the system meets these minimum requirements.

| System | Minimum requirements |
|---|---|
| Computer | • 2.33 GHz processor dual core with 4 GB RAM<br>• DVD drive<br>• Video card and monitor capable of 1280 × 1024 resolution<br>• 5 GB available on drive C<br>• NTFS format |
| Software (supported or required) | • Microsoft Windows 7 Professional SP1 (32-bit or 64-bit)<br>• Microsoft Excel™ 2007 SP2 (32-bit only) or Apache™ OpenOffice™ 4.0.1<br>• Microsoft .NET Framework 4.0 Extended<br>• Thermo Foundation™ 3.0 SP2<br>• Thermo Xcalibur™ 3.0<br>• Adobe™ Reader™ 10.1<br>• NIST™ 2008 or NIST 2011 |

# Special Notices

Make sure you follow the special notices presented in this guide. Special notices appear in boxes.

This guide uses the following types of special notices.

**IMPORTANT** Highlights information necessary to prevent damage to software, loss of data, or invalid test results; or might contain information that is critical for optimal performance of the system.

**Note** Highlights information of general interest.

**Tip** Highlights helpful information that can make a task easier.

# Contacting Us

There are several ways to contact Thermo Fisher Scientific for the information you need.

| For Thermo Scientific™ products | Access by phone, fax, email, or website |
|---|---|
| **Technical Support** | (U.S.) Phone: 1 (800) 532-4752 Fax: 1 (561) 688-8736<br>Email: us.techsupport.analyze@thermofisher.com<br>Web—for product support, technical documentation, and knowledge bases: www.thermoscientific.com/support |
| **Customer Service** (Sales and service) | (U.S.) Phone: 1 (800) 532-4752 Fax: 1 (561) 688-8731<br>Email: us.customer-support.analyze@thermofisher.com<br>Web—for product information: www.thermoscientific.com/lc-ms<br>Web—for customizing your service request:<br>1. From any Products & Services web page, click **Contact Us**.<br>2. In the Contact Us box, complete the information requested, scroll to the bottom, and click **Send**. |
| **User Documentation** | Web—for downloading documents: mssupport.thermo.com<br>1. On the Terms and Conditions web page, click **I Agree**.<br>2. In the left pane, click **Customer Manuals**.<br>3. To locate the document, click **Search** and enter your search criteria. For Document Type, select **Manual**.<br>Email—to send feedback directly to Technical Publications: techpubs-lcms@thermofisher.com<br>Web—to complete a survey about this Thermo Scientific document: www.surveymonkey.com/s/PQM6P62 |

# Accessing the Administrator Console

The Administrator Console is available from the Tools menu in any ToxFinder application window or from the Windows™ Start menu when you install the ToxFinder application.

Follow these procedures:

- To log in to the Administrator Console when user security is not enabled
- To log in to the Administrator Console when user security is enabled

### ❖ To log in to the Administrator Console when user security is not enabled

1. Do one of the following:

   - Choose **Start > All Programs > Thermo ToxFinder > ToxFinder Administration Console**.

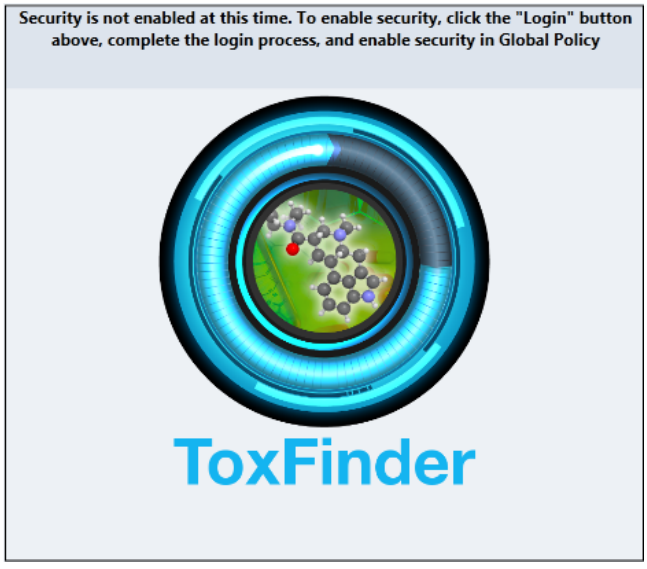
   –or–

   - Choose **Tools > Administrator Console** from the ToxFinder main menu.

   –or–

   - Double-click the **ToxFinder Administration Console** icon on your desktop, .

   The ToxFinder Administrator Console window opens, notifying you that user security is not enabled.

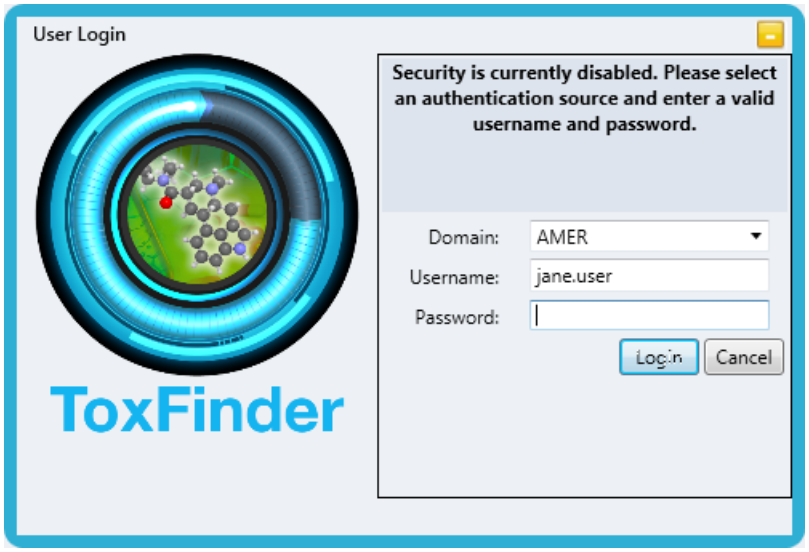

Security is not enabled at this time. To enable security, click the "Login" button above, complete the login process, and enable security in Global Policy
ToxFinder

   You can proceed without enabling user security and still have access to all Administrator Console features except the Security features.

2. To access the Security features, do the following:

   a. Click **Login**.

   The User Login dialog box opens.




   **Note** You must enter a valid user name and password before you can access the Security features.

   b. Select your domain, either your Windows Active Directory™ domain or your local windows computer name.

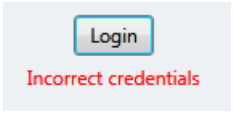
   c. Type your user name.

   d. Type your password.

   e. Click **Login**.

      The application authenticates your login and password and opens the ToxFinder Administrator Console.

      If the authentication fails, the application displays Incorrect Credentials.




      The error might be with any of the login parameters. Enter your user name and password again, or contact your system administrator.

3. To turn on user security, requiring all users to log in each time they launch the ToxFinder application, see "To enable security" on page 3.

### ❖ To log in to the Administrator Console when user security is enabled

1. Do one of the following:

   - Choose **Start > All Programs > Thermo ToxFinder > ToxFinder Administration Console**.

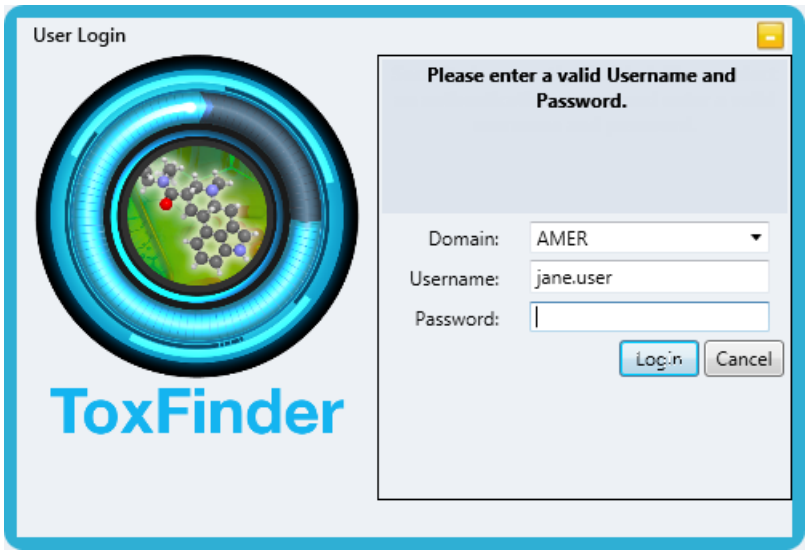
   –or–

   - Choose **Tools > Administrator Console** from the ToxFinder main menu.

   –or–

   - Double-click the **ToxFinder Administration Console** icon on your desktop, .

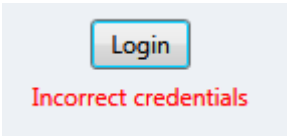
   The ToxFinder Administrator Console window opens to the User Login page.




2. Select your domain, either your Windows Active Directory domain or your local windows computer name.
3. Type your user name.
4. Type your password.
5. Click **Login**.

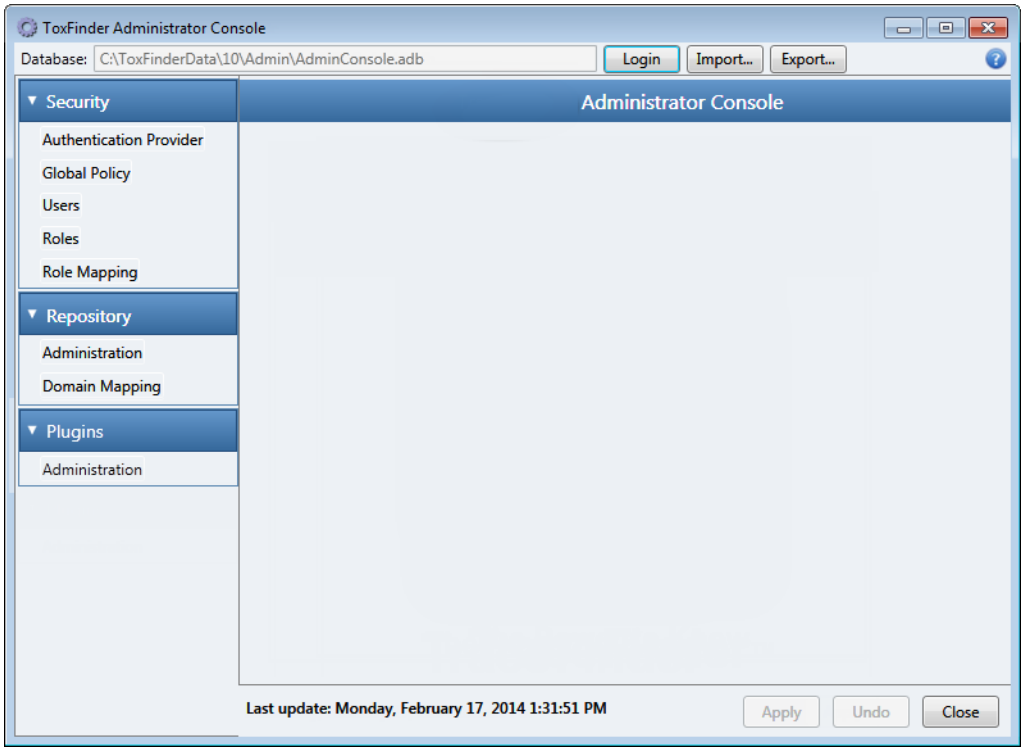
   The application authenticates your login and password and opens the ToxFinder Administrator Console.

   If the authentication fails, the application displays Incorrect Credentials.




   The error might be with any of the login parameters. Enter your user name and password again, or contact your system administrator.

## Administrator Console




You can access the following functions of the Administrator Console from the left navigation pane and the top menu bar.

| Function | Description |
|---|---|
| Security | Use the Security view to specify how the application manages authentication, to create and manage users, to map groups to roles and roles to users, or to select specific permissions for all user roles. See Chapter 1, "Using the Security View." |
| Repository | Use the Repository view to specify repositories for batches, methods, or templates that you create. See Chapter 2, "Using the Repository View." |
| Plugins | Use the Plugins view to configure available plugins for the ToxFinder application. See Chapter 3, "Using the Plugins View." |
| Import/Export | Use the Export button to save your current security settings to a file.<br><br>Use the Import button to import saved security settings to your current Administrator Console.<br><br>See Chapter 4, "Importing and Exporting Administrator Settings." |

1

# Using the Security View

When security is enabled, a user with Security permission can choose authentication providers, specify how the application manages authentication, create and manage users, map groups to roles and roles to users, and select specific permissions for all user roles.

**Contents**


- Authentication Provider
- Global Policy
- Users
- Roles
- Role Mapping


## Authentication Provider

Use the features on the Security – Authentication Provider page to select a method for authenticating user security.

### ❖ To specify how user authentication is implemented

1. Click **Authentication Provider** in the navigation pane.

   The Security – Authentication Provider page opens.

Security - Authentication Provider
Authentication Provider
Local Windows
Active Directory Domain AMER
Select...
Active Directory authentication queries the local Active Directory to perform security authentication operations. Groups or users which are mapped to application roles must exist as Active Directory user or group objects.

   The application displays the current authentication provider.

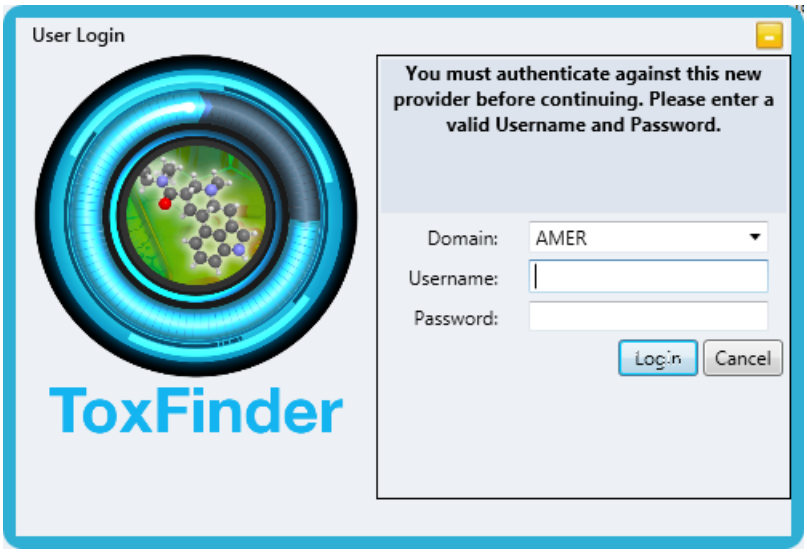
   - **Local Windows**: Uses the local Windows user login and password to allow access to the ToxFinder application. To be allowed access, users must have a Windows user account on the local machine.

- **Active Directory Domain**: Uses the selected Active Directory domain to allow access to the ToxFinder application. To be allowed access, users must be members of the selected domain.

To activate these options for user authentication, you must enable security on the Security – Global Policy page. See Global Policy.

2. To choose a different authentication provider, click **Select**.

   The User Login dialog box opens.




3. Select a domain.
4. Type your user name and password for the selected domain.
5. Click **Login**.

   The application authenticates the specified domain, user name, and password. If the authentication fails, enter your user name and password again or click **Cancel** to remain logged in to the current domain.

# Global Policy

Use the features on the Security – Global Policy page for controlling user security, automatic logoff, and access to the ToxFinder application.

Follow these procedures:

- To open the Global Policy page
- To enable security
- To enable automatic screen locking
- To restrict access only to users created in ToxFinder
- To allow access without logging in

### ❖ To open the Global Policy page

Click **Global Policy** in the navigation pane.

The Security – Global Policy page opens. For detailed descriptions of all the global policy parameters, see "Security – Global Policy Page" on page 5.

### ❖ To enable security

1. Select the **Enable Security** check box.

   The application enables the features in the Security view.

2. Click **Apply**.

   When you enable user security, users must log in with their user name and password. The application uses the authentication method you specify to authenticate the user name and password.

### ❖ To enable automatic screen locking

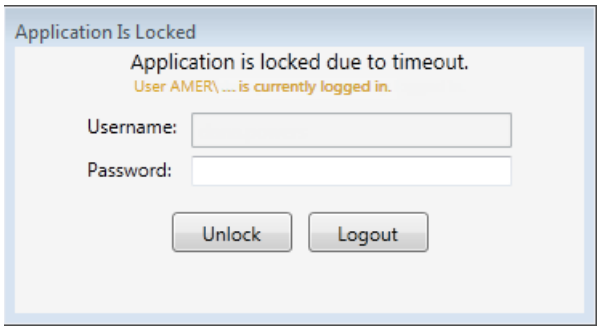
1. Select the **Lock Client...** check box.

   **Note** This feature is available only when you select the **Enable Security** check box.

2. In the Minutes box, type the number of minutes of inactivity before the application locks the screen and prompts the user to reenter the password.

   You can enter a number between 1 and 999 minutes. (999 minutes is approximately 16 hours.)

After the specified number of minutes elapses with no activity from a user, the ToxFinder application displays a lock screen with this login box.




While the password-protected lock screen is active, the ToxFinder application continues to perform all queued processing or reporting functions.

3. When you have completed all your changes to the Security – Global Policy page, click **Apply**.

### ❖ To restrict access only to users created in ToxFinder

1. Select the **Authenticate Explicit Users Only** check box.

   **Note** This feature is available only when you select the **Enable Security** check box.

2. Click **Apply**.

   The ToxFinder application allows access only to users listed in the Users list on the Users page. See "Users" on page 6. Users cannot access the application simply by being included in a local Windows security group or Active Directory.

### ❖ To allow access without logging in

1. Select the **Silent Authentication** check box.

   **Note** This feature is available only when you select the **Enable Security** check box.

2. Click **Apply**.

   Even when user security is enabled, a user who is currently logged in to a local machine can access the ToxFinder application without logging in again. The ToxFinder application authenticates the user without requiring a user name and password.

## Security – Global Policy Page

From the Security – Global Policy page, you can set parameters for user security, automatic logoff, and access to the ToxFinder application.

**Figure 1.** Security – Global Policy page

Security - Global Policy
Enable Security
Lock client that has no interaction for 5 minutes.
After lockout, the current user can log back in or log out.
Authenticate explicit users only.
Authenticate only those users who are explicitly listed under Users tab.
Silent authentication
Use current Windows user. The application will not prompt to log in.

**Table 1.** Security – Global Policy page parameters

| Function | Description |
|---|---|
| Enable Security | Turns on the user security features in the Administrator Console. |
| Lock Client that Has No Interaction… | Specifies the number of minutes before an idle ToxFinder session displays a password-protected lock screen and, unless the user enters a user name and password, automatically logs off the user.<br><br>Range: 1 through 999 minutes<br>Default: 5 minutes |
| Authenticate Explicit Users Only | Allows login access to only users listed in the Users list on the Users page. See Users. |
| Silent Authentication | With user security enabled, allows a user who is currently logged in to a local machine to access the ToxFinder application without logging in again. |

# Users

When security is enabled, use the features on the Security – Users page to create users, assign roles to users, manage role permissions, and map Active Directory groups to ToxFinder roles.

Follow these procedures:

- To open the Users page
- To add a new user
- To remove a user
- To verify a user's group membership

### ❖ To open the Users page

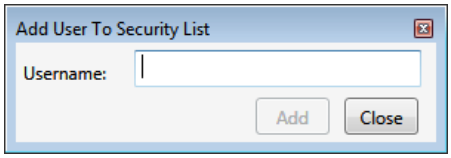
Click **Users** in the navigation pane.

The Security – Users page opens.

### ❖ To add a new user

1. Click the **Add User** icon, .

   The Add User to Security List dialog box opens.




2. Type the login name of the new user and click **Add**.
3. The application adds the new, unverified, user to the Users list.
   - A green check, , indicates verified users.
   - A red X, , indicates unverified users.
4. To verify that the users in the list are members of the current authentication group, click the **Verify Users** icon, .
5. In the Roles Granted Directly area, select the roles you want to assign to this user.
6. When you have completed all your changes, click **Apply**.

❖ **To remove a user**

1. Select the user name in the Users list.
2. Click the **Delete User** icon, .

   The application immediately removes the selected user.

❖ **To verify a user's group membership**

1. Select the user name in the Users list.
2. Click the **Refresh Groups** icon, , in the Roles Via Group Membership area.

   The application displays all groups to which the selected user belongs.

# Roles

Use the features on the Security – Roles page to define the roles that are available for users and assign permissions to these roles. This section describes the default responsibilities for the following default user roles created in the ToxFinder application: Security, LabDirector, ITAdmin, Supervisor, QAQC, and Technician. Each role has default permissions. See "Role Permission Defaults" on page 13. If your team has changed these default permissions, your access might be different. You must also activate user security for these user roles to take effect.

A user in either the default LabDirector or ITAdmin role assigns you to a role that gives you access to specific views and features of the ToxFinder application. When you log in, the navigation pane displays links to only the views, interface areas, and features that you have permission to access.

**IMPORTANT** User roles are in effect only when user security is activated. When user security is not activated, all users have access to all permissions except Security.

This section includes the following topics:


- Security
- LabDirector
- ITAdmin
- Supervisor
- QAQC
- Technician


## Security

In the Security role, you can access only the Security features on the Administrator Console; you cannot access the ToxFinder application.

## LabDirector

In the default LabDirector role, you review graphically applicable data and manipulate data, batches, methods, and instruments.

A laboratory director is responsible for these tasks:

- Creating or editing methods for new levels of detection or adding new compounds to the existing database
- Reviewing data from the mass spectrometer
- Processing samples and reviewing data collected by others
- Reporting the data
- Understanding the results and giving final approval of the released data before archiving

## ITAdmin

In the default ITAdmin role, you set security, manage users into their roles, and manipulate the various databases. You are responsible for adding compounds into the compound databases.

An IT administrator is responsible for these tasks:

- Handling the databases
- Applying roles to users
- Understanding security, users, and groups
- Creating local users and network groups

## Supervisor

In the default Supervisor role, you are responsible for setting up samples and using previously built sequences and methods for processing data. You also develop and edit methods for processing data, review the data, and distinguish between the need to reprocess samples or pass reports up to the laboratory manager for final review. On a daily basis, you establish the priority for a list of samples to run and create the sequence of events.

A supervisor is responsible for these tasks:

- Creating and submitting batches
- Reporting the data to management
- Creating or editing methods for new levels of detection or adding new compounds to the existing database
- Reviewing data from the mass spectrometer
- Understanding the results, who ran the batch, and who passed along the results before giving intermediate approval and sending the data to management
- Modifying new compounds or adjusting methods for specific result sets

## QAQC

In the default QAQC role, you review graphically applicable data and interpret the data, but you do not manipulate the data.

A QAQC technician is responsible for these tasks:

- Reviewing data from the mass spectrometer
- Understanding the results and who ran and passed along the results before giving intermediate approval and sending the data to management
- Receiving instructions for new sets of samples for the ToxFinder application to analyze after finishing the current process

**Note** In the QAQC role, you have access only to the Data Review view.

## Technician

In the default Technician role, you are responsible for setting up the instrument samples and using previously built sequences and methods for processing data. You also edit existing methods for processing data, review collected data, and distinguish between the need to reprocess samples or pass reports up to the supervisor. On a daily basis, you are responsible for gathering the list of samples to run and creating the sequence of events.

A technician is responsible for these tasks:

- Creating and submitting batches
- Creating data to be reviewed by management
- Receiving instructions for new sets of samples for the ToxFinder application to analyze after finishing the current process
- Reviewing data from the mass spectrometer
- Understanding the resulting data, making integration changes, and passing those changes up for further approval

# Using the Roles Page

Use the Security – Roles page to create new roles, change the permissions assigned to roles, or delete roles.

Follow these procedures:

- To open the Roles page
- To add a role
- To remove a role
- To change permissions for a role

### ❖ To open the Roles page

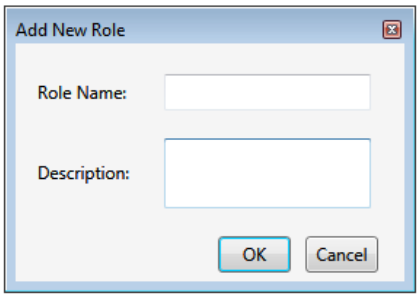
Click **Roles** in the navigation pane.

The Security – Roles page opens. For detailed descriptions of all the parameters on the Roles page, see "Security – Roles" on page 12.

### ❖ To add a role

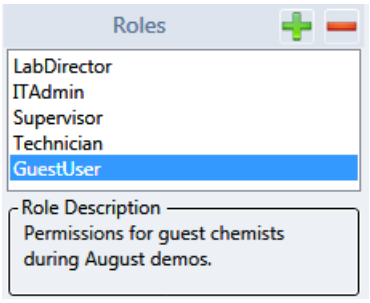
1. Click **Add Role** in the Roles area.

   The Add New Role dialog box opens.




2. In the Role Name box, type a name for the new role.
3. (Optional) In the Description box, type a description for the new user role.

   The application displays the description for a selected role below the Roles list on the Security – Roles page, as in this example:



4. Click **OK**.
5. On the Security – Roles page, select the permissions for the new role.
6. When you have made all your changes, click **Apply**.

**Note** You cannot open a different page in the Administrator Console while these changes are pending.

### ❖ To remove a role

1. Select the role in the Roles list.
2. Click the **Delete Role** icon, .
3. When prompted to confirm this action, click **Yes**.

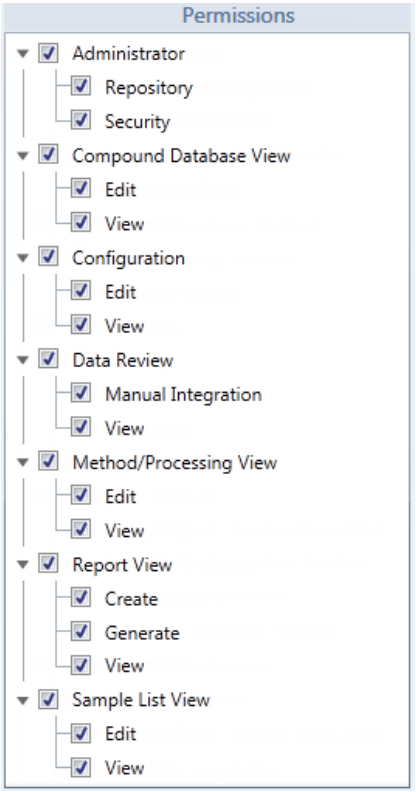
   The application immediately deletes the specified role. There is no undo for this action.

**IMPORTANT** You cannot delete the Security role. You must have at least one user role that can control security.

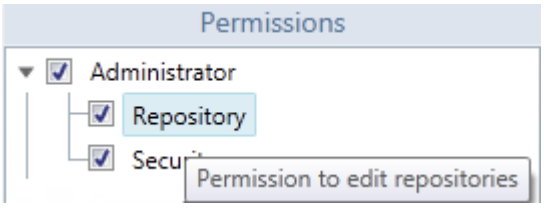
### ❖ To change permissions for a role

1. Select the role in the Roles list.

   The Permissions list indicates all the permissions assigned to the selected role. The following example shows the default permissions for the LabDirector role:



2. Select the check box for each permission you want to assign to the selected role, or clear the check box for each permission you do not want to assign to the role.
3. To see additional information about a permission, hold your cursor over the permission in the Permissions list.




4. To reset all the permissions that were specified before you made changes, click **Undo**.

   The applications discards all pending changes to all the roles.
5. When you have made all your changes, click **Apply**.

   The application saves all pending changes to all the roles.

## Security – Roles

Use the features on the Security – Roles page to create new roles, change the permissions assigned to roles, or delete roles.

**Figure 2.** Security – Roles page

**Table 2.** Roles page

| Function | Description |
|---|---|
| Roles | Displays all available roles. |
| Role Description | User-defined description of the selected role. |
| Permissions | Displays all permissions allowed for the selected role. |
| Mapped Security Groups | Displays all Windows security groups that are mapped to the selected role. The group inherits all permissions of the roles to which it is mapped. To map a security group to a role, see "Role Mapping" on page 14. |

## Role Permission Defaults

The following tables shows the default permissions assigned to each of the default user roles.

**Table 3.** Permission defaults

| Permission | LabDirector | Supervisor | ITAdmin | QAQC | Technician |
|---|---|---|---|---|---|
| **Administrator** | | | | | |
| Repository | ✓ | ✓ | ✓ | | |
| Security | ✓ | | ✓ | | |
| **Compound Database View** | | | | | |
| Edit | ✓ | ✓ | | | |
| View | ✓ | ✓ | | ✓ | ✓ |
| **Configuration** | | | | | |
| Edit | ✓ | ✓ | | | |
| View | ✓ | ✓ | | ✓ | |
| **Data Review** | | | | | |
| Manual Integration | ✓ | ✓ | | | ✓ |
| View | ✓ | ✓ | | ✓ | ✓ |
| **Method/Processing View** | | | | | |
| Edit | ✓ | ✓ | | | |
| View | ✓ | ✓ | | ✓ | ✓ |
| **Report View** | | | | | |
| Create | ✓ | ✓ | | | |
| Generate | ✓ | ✓ | | | ✓ |
| View | ✓ | ✓ | | ✓ | ✓ |
| **Sample List View** | | | | | |
| Edit | ✓ | ✓ | | | ✓ |
| View | ✓ | ✓ | | ✓ | ✓ |

**IMPORTANT** The Security role has access only to the security features on the Administrator Console. Users who are assigned only to this role cannot access other features in the ToxFinder Administrator Console or in the main ToxFinder application.

# Role Mapping

Use the features on the Security – Role Mapping page to assign Windows security groups to the default roles or the roles you defined for the ToxFinder application.

Follow these procedures:

- To open the Role Mapping page
- To create a new mapping

### ❖ To open the Role Mapping page

Click **Role Mapping** in the navigation pane.

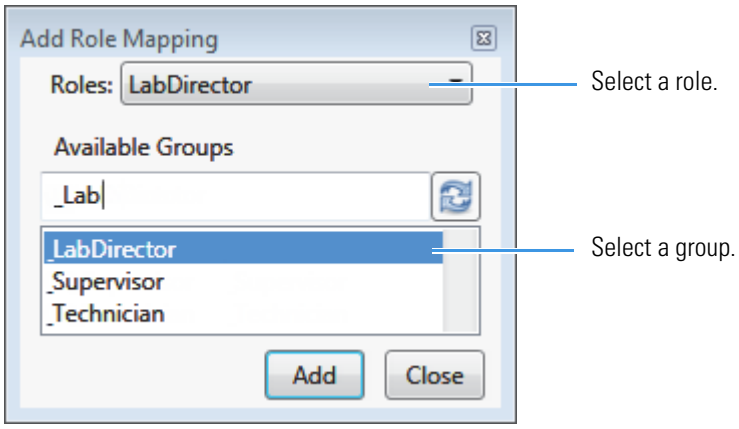
The Security – Role Mapping page opens.

Security - Role Mapping
This screen enables the application Role membership to be managed via Active Directory or local security.
Adding a user to an active directory or local group that is mapped to an application role places that user into the corresponding application role.
Likewise, removing a user from an active directory or local group that is mapped to an application role removes any privileges from that user that are associated with the corresponding application role.
This process is immediate. You will not need to click the Apply button to make your changes.
Mappings
Application Role Name
Windows Group Name
Security
Administrators

### ❖ To create a new mapping

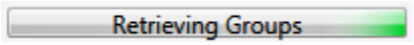
1. Click the **Create Mapping** icon, .

   The Add Role Mapping dialog box opens.



2. If the Available Groups list is not populated, click the **Retrieve Groups** icon, .

   The dialog box displays a progress bar until it finishes searching the Windows Active Directories and displays all the available groups defined for your organization.

   - A user in the default LabDirector role who also has administrator privileges on the local machine can create groups and assign users to those groups.
   - A user in the default LabDirector role who also has administrator privileges on the network can create groups in the Windows Active Directories.

3. Select a role from the Roles list.
4. Select a group from the Available Groups list.

   **Tip** This list can be very long. To quickly jump to the group you want, begin typing the group name in the text field. The list scrolls to the first matching text string. The search is not case sensitive.

5. Click **Add**.

   The application immediately creates the mapping and closes the Add Role Mapping dialog box.

6. To leave the Role Mapping page, click **Close**.

2

# Using the Repository View

Use the features in the Repository view to specify repositories for batches and methods that you create.

**Contents**


- Administration
- Domain Mapping


## Administration

Use the features on the Repository – Administration page to create and manage fixed or network drives.

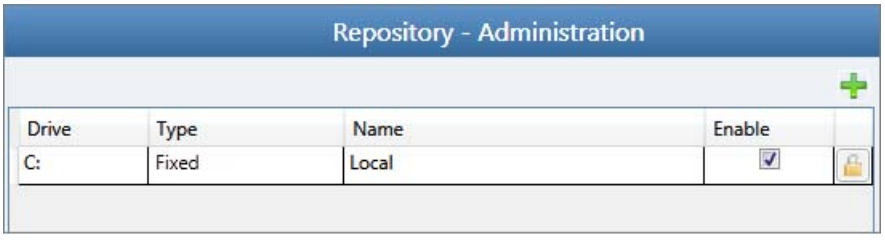
Follow these procedures:

- To open the Repository – Administration page
- To add an available repository
- To create a new repository
- To delete a repository

### ❖ To open the Repository – Administration page

Click **Administration** in the Repository navigation pane.

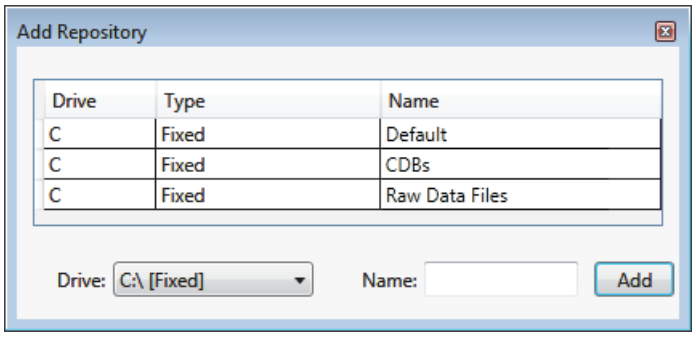
The Repository – Administration page opens.



### ❖ To add an available repository

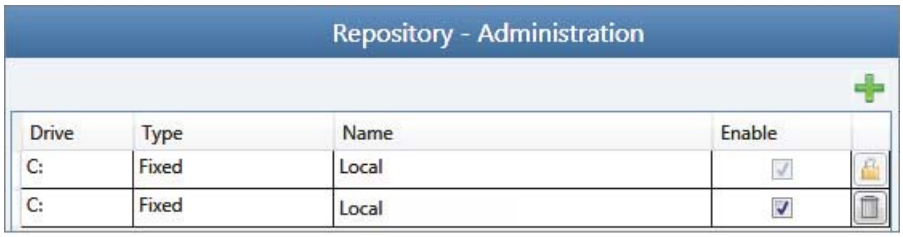
1. Click the **Add Repository** icon, .

   The Add Repository dialog box opens.




2. Select a repository in the list.
3. Click **Add**.

   The Add Repository dialog box closes, and the application adds the selected repository to the available repository list.




4. Make sure the **Enable** check box is selected.

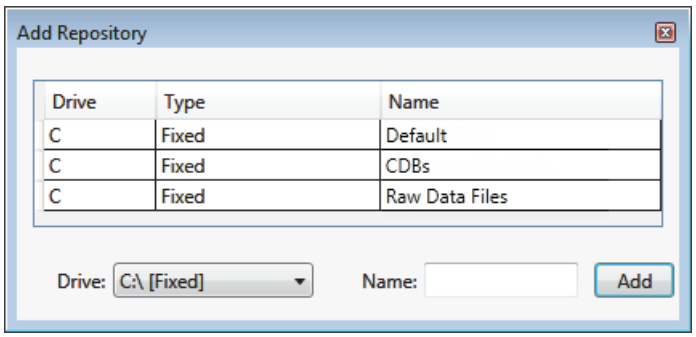
   The application enables all added repositories by default.

5. When you have made all your changes, click **Apply**.

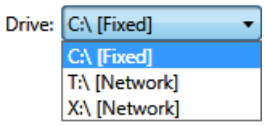
### ❖ To create a new repository

1. Click the **Add Repository** icon, .

   The Add Repository dialog box opens.



2. Select a drive from the Drive list.



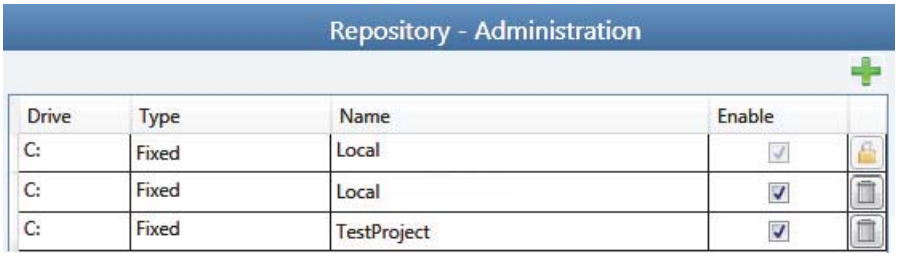

Drives can be any of the following:

- Fixed: Directly connected to your computer.
- Network: Either a remote box or a mapped drive. A shared folder that is mapped to a drive letter might physically exist on your computer, but because it is mapped, it is considered a Network drive.
- Removable: Temporary drives such as a 3.5 in. disk or a USB drive.

**Note** You cannot save data to a network or removable drive.

3. Type a name for the new repository in the Name box.
4. Click **Add**.

The Add Repository dialog box closes, and the application adds the new repository to the repository list.




5. When you have made all your changes, click **Apply**.

### ❖ To delete a repository

Next to the repository that you want to delete, click the **Remove Repository** icon, .

The application immediately removes the repository. There is no confirmation.

**Note** Using the Undo function does not necessarily return a deleted repository. The Undo function returns the Repository – Administration page to the state when you first opened it or to the state immediately after the last Apply.

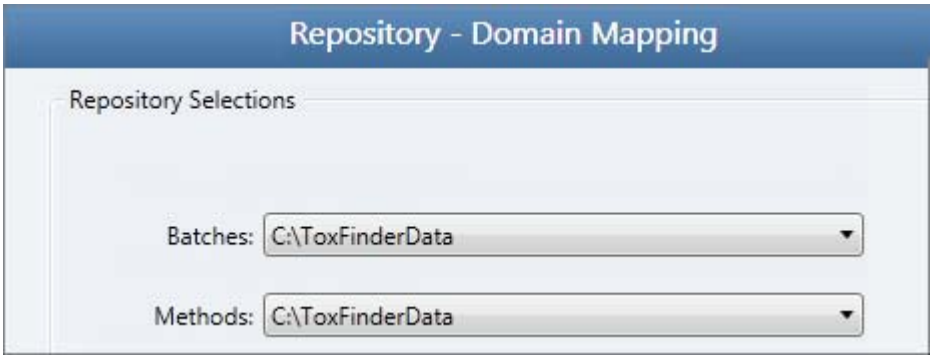
# Domain Mapping

Use the domain mapping features to change the drive where you store your data folders, such as batches and methods (the default location is C:\ToxFinderData). You must use a fixed drive. You cannot save data to a network or removable drive.

### ❖ To select the drives for storing data folders

1. Click **Domain Mapping** in the Repository navigation pane.

   The Repository – Domain Mapping page opens.




2. Select a domain.
3. In the Repository Selections area, select the repository where you want to save batches and methods.

   The dropdown lists display the default repository and all available repositories that you added. See "To add an available repository" on page 18 or "To create a new repository" on page 18.

   By default, the application saves batches and methods to the following folders:

   C:\ToxFinderData\1.0\Projects

   C:\ToxFinderData\1.0\Methods

   When you create any of these items in the ToxFinder application, the application creates Projects and Methods folders in your specified repositories.

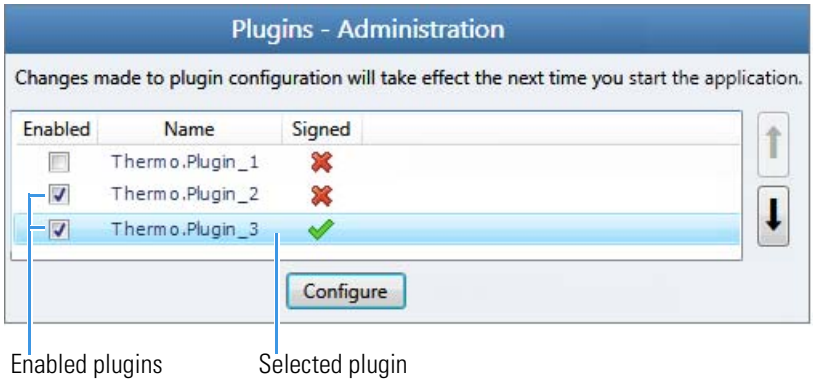
# Using the Plugins View

Use the features on the Plugins – Administration page to configure available plugins for the ToxFinder application.

### ❖ To enable plugins

1. Click **Administration** in the Plugins navigation pane.

   The Plugins – Administration page opens, listing all available plugins.




2. For each plugin that you want to use in the ToxFinder application, select the **Enabled** check box.

3. To configure a plugin, select the plugin and click **Configure**.

   **Note** You can configure only one plugin at a time. Do not confuse an *enabled* plugin with a *selected* plugin.

   A dialog box for the selected plugin opens.

4. In the configuration dialog box, select the options you want to configure and then click **Save**.

5. Click **Apply**.

   The enabled plugins become available the next time you start the ToxFinder application.

4

# Importing and Exporting Administrator Settings

Use the Export button to save your current security settings to a file.

Use the Import button to import saved security settings to your current Administrator Console.

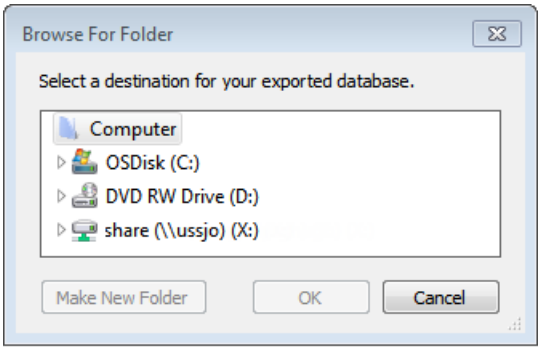
Follow these procedures:

- To export settings to a file
- To import settings from a file

### ❖ To export settings to a file

1. Set and apply all the settings that you want to export.
2. Click **Export**.

   The Browse For Folder dialog box opens.




3. Locate the folder where you want to save the exported file and click **OK**.

   The target folder can be on the local machine, on a network drive, or on a USB drive.

   **Tip** To create a new folder for the saved data, navigate to a higher level folder, click **Make New Folder**, type the name for the new folder, and click **OK**.

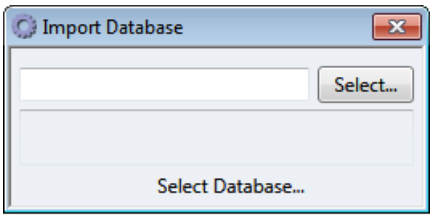
   The application writes the saved security information to the following file:

   AdminConsole.abd

### ❖ To import settings from a file

1. Click **Import**.

   The Import Database dialog box opens.

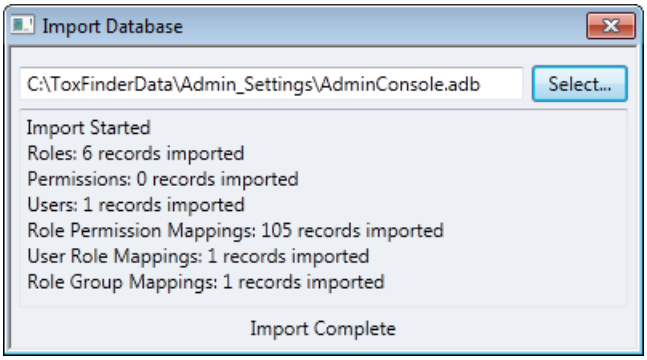



2. Click **Select** and locate a saved administrator database file (.adb) to import.

   The database file can be on the local machine, on a network drive, or on a USB drive.

3. Click **Open**.

   The Import Database dialog box displays the imported records.




4. Close the Import Database dialog box.
5. To see the imported changes on your current page, refresh the page.

# Index


## A

Active Directory Domain, authentication method 2
AdminConsole.abd 23
authentication, user security 1
automatic screen locking 3

## C

contacting us vii

## D

domain mapping 20

## E

exporting administrator settings 23

## I

importing administrator settings 24
ITAdmin role 8

## L

LabDirector role 8
Local Windows, authentication method 1
logging in
  when user security is enabled x
  when user security is not enabled viii

## M

mapping, roles 14

## P

Plugins – Administration page 21
procedures
  add a new user 6
  add a role 10
  add an available repository 18
  allow a single-access login 4
  change permissions for a role 11
  create a new mapping 14
  create a new repository 18
  delete a repository 19
  enable automatic screen locking 3
  enable plugins 21
  enable security 3
  export settings to a file 23
  import settings from a file 24
  open the Administration page 17
  open the Global Policy page 3
  open the Role Mapping page 14
  open the Roles page 10
  open the Users page 6
  open ToxFinder Administrator Console Help v
  remove a role 11
  remove a user 7
  restrict access only to users created in ToxFinder 4
  select the drives for storing data folders 20
  specify how user authentication is implemented 1
  verify a user's group membership 7
  view ToxFinder documents using the Start menu v

## Q

QAQC role 9

## R

Repository – Administration page 17
Repository – Domain Mapping page 20
role mapping 14
role permission defaults 13
roles
  ITAdmin 8
  LabDirector 8
  QAQC 9
  Security 7
  Supervisor 8
  Technician 9

## S

screen locking, automatic 3
Security – Authentication Provider page 1
Security – Global Policy page 5
Security – Role Mapping page 14
Security – Roles page 10
Security – Users page 6
Security role 7
Supervisor role 8
system requirements vi

## T

Technician role 9

## U

user security, enabling 3